Zur Gaußischen Theorie der Reduktion binärer quadratischer Formen.

Von L. RÉDEI in Szeged.

In der Theorie der Äquivalenz der binären quadratischen Formen ist wohl der schwierigste Punkt der Nachweis, daß im Fall einer positiven Determinante äquivalente reduzierte Formen derselben Periode angehören. Aus diesem Satz folgt, daß die Klassenzahl gleich der Anzahl der Perioden ist. Eine nicht weniger wichtige Folgerung ist, daß die Perioden die Fundamentallösung der Pellschen Gleichung liefern; bis heute gibt es keine einfachere Methode zum Auffinden aller Lösungen dieser Gleichung.

GAUSZ[1]) hat den genannten Satz mit Hilfe von Kettenbrüchen bewiesen. Auf dieses fremde Mittel haben auch die späteren Autoren nicht verzichtet, obwohl eine Bestrebung vorlag, die Theorie eben in diesem Punkt zu vereinfachen. Im Gegenteil hat DIRICHLET[2]) eine Vereinfachung unter anderem dadurch erreicht, daß er die Theorie der Kettenbrüche noch mehr zur Geltung brachte. Man sehe auch die Lehrbücher von CAHEN[3]) und DICKSON[4]).

Hier möchte ich einen Beweis mitteilen, der frei von Kettenbrüchen und auch sonst einfacher ist, als die bisherigen Beweise. Kurz werde ich auch darauf hinweisen, daß man dann auch bei der Anwendung auf die Pellsche Gleichung ohne Kettenbrüche auskommt.

---

[1]) C. F. GAUSZ, *Werke*, I (Leipzig, 1870), S. 180.

[2]) L. DIRICHLET—R. DEDEKIND, *Vorlesungen über Zahlentheorie*, 4. Aufl. (Braunschweig, 1894), S. 199.

[3]) E. CAHEN, *Théorie des nombres*, II (Paris, 1924), p. 305.

[4]) L. E. DICKSON—E. BODEWIG, *Einführung in die Zahlentheorie* (Leipzig und Berlin, 1931), S. 103.

Die Kenntnis des einschlägigen Kapitels im angeführten Lehrbuch von DIRICHLET setze ich voraus, übernehme auch die Bezeichnung fast unverändert, fühle mich trotzdem gezwungen, bequemlichkeitshalber einiges vorangeschickt zu wiederholen.

Unter einer binären quadratischen Form (kurz Form) verstehen wir mit GAUSZ

$$\varphi = ax^2 + 2bxy + cy^2$$

mit ganzen rationalen Koeffizienten a, b, c.[5]) Die Determinante $D = b^2 - ac$ soll stets positiv und keine Quadratzahl sein. Wir nennen

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad (\alpha\delta - \beta\gamma = 1)$$

mit rationalen $\alpha, \beta, \gamma, \delta$ eine Substitution. Unter $S\varphi$ werde die Form $ax'^2 + 2bx'y' + cy'^2$ verstanden, wobei $x' = \alpha x + \beta y$, $y' = \gamma x + \delta y$ ist. Gilt eine Beziehung $\psi = S\varphi$, so heißen φ und ψ äquivalent. Die Substitutionen

$$E = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$$

heißen elementar, die $E\varphi$ die Nachbarformen von φ. Es gibt nur ein E, die φ in eine gegebene Nachbarform überführt.

Erste bzw. zweite Wurzel von φ sind durch

$$\omega = \frac{-b - \sqrt{D}}{c}, \quad \omega' = \frac{-b + \sqrt{D}}{c}$$

definiert, wobei wir $\sqrt{D}$ positiv annehmen. D und ω bestimmen die Form φ eindeutig. Sind $\overline{\omega}, \overline{\omega}'$ die entsprechenden Wurzeln einer zweiten Form $\overline{\varphi}$, so sind

$$(1) \qquad \overline{\varphi} = S\varphi, \quad \omega = \frac{\gamma + \delta\overline{\omega}}{\alpha + \beta\overline{\omega}}, \quad \omega' = \frac{\gamma + \delta\overline{\omega}'}{\alpha + \beta\overline{\omega}'}$$

gleiche Aussagen. Insbesondere sind φ und $\overline{\varphi}$ Nachbarformen dann und nur dann, wenn

$$(2) \qquad \omega + \frac{1}{\overline{\omega}} = r \qquad (r \text{ ganz rational})$$

ist, und zwar ist dann $\overline{\varphi} = \begin{pmatrix} 0 & 1 \\ -1 & r \end{pmatrix}\varphi$.

[5]) Ich wollte mich auch in dieser Hinsicht an Dirichlets Lehrbuch anpassen, obwohl bekanntlich Lagranges Definition $\varphi = ax^2 + bxy + cy^2$ sich mit der Zeit für glücklicher erwies. Unsere Arbeit läßt sich aber ohne jede Mühe für Lagranges Definition umschreiben.

Reduziert heißt φ, wenn

$$|\omega| > 1, \quad |\omega'| < 1, \quad \omega\omega' < 0 \tag{3}$$

ist. Nachher werden nur noch reduzierte Formen betrachtet. Unter ihnen hat jedes φ eine einzige Nachbarform $\overline{\varphi}$, und das entsprechende E (nämlich das mit $E\varphi = \overline{\varphi}$) ist durch

$$\delta = \{\omega\} \tag{4}$$

bestimmt, wobei $\{\omega\}$ die ganze rationale Zahl zwischen 0 und ω bedeutet, die zu ω am nächsten liegt. (Wie hier, so auch später wollen wir mit „zwischen u und v" u und v selbst ausschließen. (4) ist sinnvoll, da $|\omega| > 1$ ist.)

Geht man also von einer reduzierten Form $\varphi = \varphi_1$ aus, so erhält man durch fortgesetzte Bildung von reduzierten Nachbarformen eine eindeutig bestimmte unendliche Folge $\varphi_1, \varphi_2, \varphi_3, \ldots$, die wir die Kette von φ nennen. Stets soll E_i die elementare Substitution bezeichnen, für die $E\varphi_i = \varphi_{i+1}$ ist. Jede Kette wiederholt sich periodisch, d. h. es gibt ein ganzes m so, daß $\varphi_1, \varphi_2, \ldots, \varphi_m$ verschieden sind, dagegen $\varphi_i = \varphi_k$ für $i \equiv k \pmod{m}$ gilt. $\varphi_1, \varphi_2, \ldots, \varphi_m$ heißt die Periode von φ, m die Periodenzahl.

Wir definieren noch $-S = \begin{pmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{pmatrix}$. Es sollen also S und $-S$ als verschieden betrachtet werden, obzwar immer $S\varphi = (-S)\varphi$ ist. Wir beweisen den Satz:

Es sei $\mathfrak{S} = (S, \varphi, \overline{\varphi})$ ein „System" bestehend aus einer Substitution $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ und zwei reduzierten Formen $\varphi, \overline{\varphi}$ mit $S\varphi = \overline{\varphi}$. Abgesehen vom trivialen Fall $S = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ gilt genau eine der Gleichungen

$$\operatorname{sgn} \overline{\omega} = \operatorname{sgn} \gamma\delta, \tag{5_1}$$

$$\operatorname{sgn} \omega = -\operatorname{sgn} \alpha\gamma, \tag{5_2}$$

wobei $\operatorname{sgn} z = \frac{z}{|z|}$ $(z \neq 0)$ ist. Gilt (5_1), so ist $S = \pm E_1 E_2 \ldots E_n$ mit irgendeinem n, zugleich also $\overline{\varphi} = \varphi_{n+1}$. Gilt aber (5_2), so gilt für das „umgekehrte" System $\mathfrak{S}^{-1} = (S^{-1}, \overline{\varphi}, \varphi)$ der (5_1) entsprechende Zusammenhang (und also mit entsprechender Bezeichnung $S^{-1} = \pm \overline{E}_1 \overline{E}_2 \ldots \overline{E}_n$, $\varphi = \overline{\varphi}_{n+1}$).

Zum Beweis setzen wir

$$|S| = |\alpha| + |\beta| + |\gamma| + |\delta|. \tag{6}$$

Da für $S=\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$ nichts behauptet wird, schließen wir diesen Fall aus.

Weiter zeigen wir, daß dann $\beta\gamma=0$ unmöglich ist. Ist nämlich $\beta=0$, so ist $\alpha\delta=1$, $\gamma\neq0$, und also nach (1) $\omega=\alpha\gamma+\overline{\omega}$, $\omega'=\alpha\gamma+\overline{\omega}'$. Aus dem letzteren folgt nach (3) $\alpha\gamma=\pm1$, $\operatorname{sgn}\omega'=-\operatorname{sgn}\overline{\omega}'$, also auch $\operatorname{sgn}\omega=-\operatorname{sgn}\overline{\omega}$. Wieder nach (3) ist dann $|\omega-\overline{\omega}|>2$, und das ist wegen $\omega-\overline{\omega}=\alpha\gamma$ unmöglich. Nehmen wir jetzt $\gamma=0$ an. Dann folgt $\alpha\delta=1$, $\beta\neq0$, und nach (1) $\frac{1}{\omega}=\beta\delta+\frac{1}{\overline{\omega}}$, $\frac{1}{\omega'}=\beta\delta+\frac{1}{\overline{\omega}'}$. Jetzt folgt nach dem vorletzten Zusammenhang und (3), daß $\beta\delta=\pm1$, $\operatorname{sgn}\omega=-\operatorname{sgn}\overline{\omega}$, also auch $\operatorname{sgn}\omega'=-\operatorname{sgn}\overline{\omega}'$ ist. Nach (3) heißt das $\left|\frac{1}{\omega'}-\frac{1}{\overline{\omega}'}\right|>2$, und so ist mit $\frac{1}{\omega'}-\frac{1}{\overline{\omega}'}=\beta\delta$ wieder ein Widerspruch entstanden.

Auch noch den Fall $\alpha\delta=0$ schicken wir voran. Es werde zuerst $\alpha=0$. Dann ist $\beta\gamma=-1$, $S=\pm\begin{pmatrix}0&1\\-1&r\end{pmatrix}$ (r ganz rational). Da also $\pm S$ elementar ist, muß $\overline{\varphi}$ wegen $S\varphi=\overline{\varphi}$ gleich φ_2 und $S=\pm E_1$ sein. Nach (4) und (2) folgt hieraus $r=\{\omega\}$, $\operatorname{sgn}\overline{\omega}=-\operatorname{sgn}r$. Das bedeutet eben, daß jetzt (5_1) gilt. Endlich gilt (5_2) wegen $\alpha=0$ nicht, und so ist der Satz für diesen Fall richtig. Es werde dann $\delta=0$. Für $\mathfrak{S}^{-1}=\left(\begin{pmatrix}\delta&-\beta\\-\gamma&\alpha\end{pmatrix},\overline{\varphi},\varphi\right)$ ist das der vorige Fall. Nach dem eben Gesehenen gilt (5_1) für dieses System, d. h. $\operatorname{sgn}\omega=-\operatorname{sgn}\alpha\gamma$, und das bedeutet eben, daß für $\mathfrak{S}$ (5_2) gilt. Dagegen gilt (5_1) für $\mathfrak{S}$ wegen $\delta=0$ nicht, womit die Richtigkeit des Satzes auch für diesen Fall erwiesen ist.

Es ist nur noch der Fall $\alpha\beta\gamma\delta\neq0$ übrig. Offenbar gilt $\alpha\beta\gamma\delta>0$. Zuerst zeigen wir, daß aus (5_1) und (5_2) genau des eine gilt. Gilt nämlich (5_1), d. h. $\operatorname{sgn}\overline{\omega}=\operatorname{sgn}\gamma\delta=\operatorname{sgn}\alpha\beta$, so ist $\operatorname{sgn}\delta\overline{\omega}=\operatorname{sgn}\gamma$, $\operatorname{sgn}\beta\overline{\omega}=\operatorname{sgn}\alpha$. Hieraus und aus (1) folgt $\operatorname{sgn}\omega=\operatorname{sgn}\frac{\gamma}{\alpha}$, d. h. (5_2) gilt nicht. Gilt dagegen (5_1) nicht, ist also $\operatorname{sgn}\overline{\omega}=-\operatorname{sgn}\gamma\delta$, so folgt $\operatorname{sgn}\overline{\omega}'=\operatorname{sgn}\gamma\delta$ und weiter hieraus ebenso wie vorher $\operatorname{sgn}\omega'=\operatorname{sgn}\frac{\gamma}{\alpha}$. Dies bedeutet wirklich eben, daß (5_2) gilt.

Mit der letzten Behauptung des Satzes sind wir durch die Bemerkung fertig, daß (5_2) (für $\mathfrak{S}$) dasselbe ist wie (5_1) für $\mathfrak{S}^{-1}=\left(\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}, \overline{\varphi}, \varphi\right)$.

Wir müssen nur noch den Hauptpunkt beweisen, daß (im Fall $\alpha\beta\gamma\delta\neq 0$) aus (5_1) $S=\pm E_1E_2\dots E_n$ folgt. Das tun wir durch Induktion, indem wir die Behauptung für jeden ähnlichen Fall voraussetzen, wenn nur $|S|$ einen „kleineren" Wert hat. Wir setzen

$$r=\{\omega\}. \tag{7}$$

Nach (4) ist dann $E_1=\begin{pmatrix}0 & 1\\ -1 & r\end{pmatrix}$. Weiter setzen wir $T=E_1^{-1}S$. Wegen $\alpha\beta\gamma\delta\neq 0$ ist $T\neq\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Es ist $T\varphi_2=T(E_1\varphi)=S\varphi=\overline{\varphi}$, und das heißt, daß auch $\mathfrak{T}=(T, \varphi_2, \overline{\varphi})$ ein System ist. Zeigen wir, daß auch für dieses Fall (5_1) vorliegt und $|T|<|S|$ ist, so folgt hieraus $T=\pm E_2E_3\dots E_n$ $(n\geqq 2)$ entweder nämlich nach der Voraussetzung oder nach dem schon bewiesenen Fall $\alpha\beta\gamma\delta=0$ des Satzes. Dann folgt weiter $S=E_1T=\pm E_1E_2\dots E_n$, und so werden wir den Satz auf diesem Wege bewiesen haben.

Nun ist

$$T=\begin{pmatrix}r & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix},$$

also

$$T=\begin{pmatrix}\gamma' & \delta'\\ \alpha & \beta\end{pmatrix} \quad \text{mit} \quad \gamma'=\alpha r-\gamma,\ \delta'=\beta r-\delta. \tag{8}$$

Aus (5_1) folgt aber $\operatorname{sgn}\overline{\omega}=\operatorname{sgn}\alpha\beta$, und dies bedeutet eben, daß (5_1) auch für $\mathfrak{T}$ gilt.

Um die Restbehauptung $|T|<|S|$ zu beweisen, schreiben wir (1) in der Form

$$\omega=\frac{\gamma}{\alpha}+\frac{\overline{\omega}}{\alpha(\alpha+\beta\overline{\omega})}=\frac{\delta}{\beta}-\frac{1}{\beta(\alpha+\beta\overline{\omega})}.$$

Wie eben erwähnt, ist $\operatorname{sgn}\overline{\omega}=\operatorname{sgn}\alpha\beta$, und so folgt, daß ω zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ liegt. Wegen (7) ist wenigstens das eine von $\left|r-\frac{\gamma}{\alpha}\right|$ und $\left|r-\frac{\delta}{\beta}\right|$ kleiner als 1. Wäre das andere größer als 1, so läge eine ganze rationale Zahl (nämlich $r+1$ oder $r-1$) zwischen

$\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$. Hieraus folgt, daß es zwischen $\beta\gamma$ und $\alpha\delta$ ebenfalls eine ganze rationale Zahl liegt, das doch wegen $\alpha\delta = \beta\gamma + 1$ unmöglich ist. Also ist immer

$$\left| r - \frac{\gamma}{\alpha} \right| \leqq 1, \quad \left| r - \frac{\delta}{\beta} \right| \leqq 1,$$

und es gilt hier wenigstens ein Zeichen $<$. Nach Multiplizieren mit $|\alpha|$ bzw. $|\beta|$ und Addieren folgt wegen (8)

$$|\gamma'| + |\delta'| < |\alpha| + |\beta|. \tag{9}$$

Nach Obigem muß wegen $|\omega| > 1$ wenigstens das eine von $\left|\frac{\gamma}{\alpha}\right|$ und $\left|\frac{\delta}{\beta}\right|$ größer als 1 sein. Wäre das andere kleiner als 1, so würde wieder die Unmöglichkeit folgen, daß zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ eine ganze rationale Zahl liegt. Also ist

$$|\alpha| + |\beta| < |\gamma| + |\delta|.$$

Dies mit (8) und (9) ergibt $|T| < |S|$, womit der Satz bewiesen ist.

Unser Satz enthält den obigen Satz von GAUSZ offenbar. Wir zeigen noch, wie man aus unserem Satz (wie gesagt, ebenfalls ohne Kettenbrüche) zur Fundamentallösung der Pellschen Gleichung

$$t^2 - Du^2 = 1 \tag{10}$$

kommt. Der Spezialfall $\overline{\varphi} = \varphi$ ergibt nämlich, daß alle Substitutionen S, die eine reduzierte Form φ in sich überführen, durch

$$S = \pm (E_1 E_2 \ldots E_m)^i \qquad (i = 0, \pm 1, \pm 2, \ldots) \tag{11}$$

angegeben sind. Diese und die Lösungen von (10) stehen miteinander in einem bekannten ein-eindeutigen Zusammenhang. Ein Teil davon ist

$$\gamma = au.$$

Die Bedingung für nicht triviale Lösungen ($u \neq 0$) von (10) lautet also, daß es unter den S in (11) eins mit $\gamma \neq 0$ gibt. Nun ist $S_0 = E_1 E_2 \ldots E_m$ ein solches, was man so beweist. Wir setzen

$$E_k = \begin{pmatrix} 0 & 1 \\ -1 & \delta_k \end{pmatrix}.$$

Dann haben $\delta_1, \delta_2, \ldots$ abwechselnde Vorzeichen. Betrachten wir z. B. den Fall $\delta_1 > 0$ (der Fall $\delta_1 < 0$ ließe sich ähnlich behandeln).

Dann sind alle vier Elemente von

$$E_1E_2=\begin{pmatrix}-1 & \delta_2\\ -\delta_1 & -1+\delta_1\delta_2\end{pmatrix}$$

von gleichem (negativem) Vorzeichen. Ähnliches gilt für E_3E_4, $E_5E_6, \ldots$ und also, da m gerade ist, offenbar auch für S_0. Das beweist schon, daß S_0 eine nicht triviale Lösung von (10) liefert. Weiter folgt, daß die Absolutwerte aller vier Elemente in S_0^i mit i monoton zunehmen, und somit entspringt aus $S=S_0$ (vom Vorzeichen abgesehen) eben die Fundamentallösung von (10).

(Eingegangen am 26. November 1941.)